UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

Andrew Greder, on behalf of himself and all others similarly situated, Plaintiff, v. Uber Technologies Inc.; Rasier, LLC; Rasier-CA, LLC, Defendants.	Case No: **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Andrew Greder ("Plaintiff"), by his undersigned counsel, for himself and all others similarly situated, hereby commences this class action suit against Defendants Uber Technologies, Inc., Rasier LLC, and Rasier-CA LLC ("Defendants"), and alleges as follows:

NATURE OF ACTION

1. In November 2017, Uber announced that over a year earlier in October 2016, hackers gained access and had stolen information relating to 57 million driver and rider accounts for the Uber rideshare service.

2. Because of this breach, Plaintiff and the millions of individuals whose personal data were exposed now face serious risk of further injury from identity theft, credit and reputational harm, false tax claims, and even extortion.

3. This action is brought on behalf of a Nationwide Class of individuals whose personal information ("Personal Data") was made available to unauthorized third parties through Defendants' negligent conduct.

4. Plaintiff and the proposed class of consumers were harmed by Defendants' inadequate data security practices. Plaintiff seeks to represent himself, a nationwide class of all consumers in the United States whose Personal Data was compromised by Defendants' actions.

5. On behalf of himself and the Class, Plaintiff seeks actual damages, statutory damages, punitive damages, and equitable and declaratory relief.

PARTIES

6. Plaintiff Andrew Greder is an individual who resides in Minnetonka, Minnesota and was a citizen of the State of Minnesota during the period of the Uber Data Breach. Plaintiff had an active account with Uber at the time of the Uber Data Breach.

7. Defendant Uber Technologies, Inc., is a California corporation with its headquarters and principal place of business located in San Francisco, California.

8. Defendant Rasier, LLC, is a California Limited Liability Company with its principal place of business in San Francisco, California.

9. Defendant Rasier-CA, LLC, is a California Limited Liability Company with its principal place of business in San Francisco, California.

10. Defendants do business nationwide, including within this District.

11. Upon information and belief, the wrongful acts and/or decisions of Defendants that led to this data breach occurred nationwide as well as in this District.

FACTUAL ALLEGATIONS

12. On November 21, 2017, Uber publicly acknowledged the existence of a massive data breach in its system that had occurred approximately a year earlier, in October 2016. 57 million users of the Uber rideshare service, including both riders and drivers, had their personal information made vulnerable to the hackers.

13. Defendants paid these hackers at least $100,000 to conceal the existence of a massive data breach.

14. The two hackers were able to gain access to information stored on GitHub, an online cloud-based service that allows collaboration between engineers in developing software code. On GitHub, the hackers were able to steal credentials for another, separate cloud services provider. From that other provider, the hackers downloaded Uber drivers' and riders' data.

15. The information stolen by hackers includes names, email addresses, and mobile phone numbers, as well as the names and license numbers of over 600,000 Uber drivers in the United States.

16. During the breach, in October 2016, Defendants were negotiating with the U.S. Federal Trade Commission over the proper handling of consumer data.

17. Despite the potential danger to their customers and drivers, Defendants delayed the disclosure of the breach until over a year after it had occurred, and took active measures to conceal that the breach had ever happened.

18. The disclosure of the 2016 breach was not the first time Defendants were accused of having inadequate security policies. Earlier in 2017, before the most recent

breach disclosure, London's transport regulator revoked Defendant Uber's license to operate in the city, citing the company's failures to deal with public safety and security.

19. Defendants hold themselves out to be sophisticated technology companies with the expertise to handle and safeguard the personal data of the users of their service.

20. The security breach of the personal data stored on Defendants' servers has created a substantially increased risk of identity theft to Plaintiff and the Class for the foreseeable future.

21. According to a 2012 report published by the Federal Trade Commission, the "range of privacy-related harms is more expansive than economic or physical harm or unwarranted intrusions," and "any privacy framework should recognize additional harms that might arise from unanticipated uses of data." There is "significant evidence demonstrating that technological advances and the ability to combine disparate pieces of data can lead to identification of a consumer, computer or device even if the individual pieces of data do not constitute [personally identifiable information]."

JURISDICTION AND VENUE

22. This Court has original jurisdiction pursuant to 28 U.S.C. § 1332(d)(2)(A). There is minimal diversity and the amount in controversy exceeds $5,000,000, exclusive of interest and costs.

23. This Court has personal jurisdiction over Defendants because they conduct significant business in the District, and the unlawful conduct alleged in the Complaint occurred in, was directed to, and/or emanated from this District.

24. Venue is proper in the District of Minnesota because Defendants regularly transacts business in this District, a substantial part of the events or omissions giving rise to the claims occurred in this District, and the Plaintiff and some of the Class Members resides in this District.

CLASS ACTION ALLEGATIONS

25. Plaintiff incorporates the allegations in each above numbered paragraph.

26. Plaintiff brings this action on behalf of himself and all others similarly situated.

27. Plaintiff seeks to represent the following Class:

Nationwide Class ("the Class")

> All persons residing in the United States or its territories whose Personal Data was accessed in the Data Breach announced on Nov. 21, 2017.

28. Excluded from the Class are:

a. Any Judge or Magistrate presiding over this action and members of their families;

b. Defendants, Defendants' subsidiaries, parents, successors, predecessors, and any entity in which Defendants or their parents have a controlling interest and their current or former employees;

c. Counsel for Plaintiff and Defendants;

d. Persons who properly execute and file timely request for exclusion from the Class;

e. Legal representatives, successors, or assigns of any such excluded persons;

f. All persons who have previously had claims finally adjudicated or who have released their claims against Defendants similar to those alleged herein; and

g. Any individual who contributed to the unauthorized access of the Defendants' database.

29. The Class members are so numerous that individual joinder of all its members is impracticable. While the precise identification of Class members is unknown to Plaintiff at this time and can be ascertained only through appropriate discovery of Defendants, the Nationwide Class is believed to number approximately 57 million.

30. This action is brought and may properly be maintained as a class action pursuant to the provisions of Federal Rules of Civil Procedure 23(a)(1)-(4) and 23(b)(1)-(3). This action satisfies the numerosity, commonality, typicality, adequacy, predominance, and superiority requirements of those provisions. Common questions of fact and law exist as to all Class members which predominate over any questions affecting only individual Class members. These common legal and factual questions, which do not vary from Class member to Class member, and which may be determined without reference to the individual circumstances of any Class member, include the following:

a. Whether Defendants owed a duty to Class Members under federal or state law to protect their Personal Data, provide timely notice of unauthorized access that personal data;

b. Whether Defendants failed to establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of the Class members' Personal Data;

c. Whether Defendants failed to ensure adequate protection against known and anticipated threats to security;

d. Whether Defendants willfully failed to design, employ, and maintain an adequate system to protect consumers' personal data;

e. Whether Defendants failed to notify consumers of the breach and/or notify them as soon as was practicable after the breach's discovery;

f. Whether Defendants' representations about their security was false or misleading;

g. Whether Defendants' deliberate concealment violated applicable state consumer protection laws; and

h. Whether Plaintiff and the Class members suffered damages; and

i. Whether Plaintiff and the Class members are entitled to injunctive, declaratory, and monetary relief as a result of Defendants' conduct.

31. Plaintiff's claims are typical of the claims of the Class members. Plaintiff and other Class members must prove the same facts in order to establish the same claims, described herein, which apply to all Class members.

32. Plaintiff is adequate representatives of the Class because he is a member of the Class and his interests do not conflict with the interests of the Class members he seeks to represent. Plaintiff has retained counsel competent and experienced in the prosecution of complex class action, data breach, and consumer privacy litigation, and together Plaintiff and his counsel intend to prosecute this action vigorously for the benefit of the Class. The interests of Class members will be fairly and adequately protected by Plaintiff and his counsel.

33. A class action is superior to other available methods for the fair and efficient adjudication of this litigation since individual litigation of the claims of all Class members is impracticable. Even if every Class member could afford individual litigation, the court system could not. It would be unduly burdensome to the courts, in which individual litigation of thousands of cases (or more) would proceed. Individual litigation presents a potential for inconsistent or contradictory judgments, the prospect of a race for the courthouse, and an inequitable allocation of recovery among those with equally meritorious claims. Individual litigation increases the expense and delay to all parties and the court system in resolving the legal and factual issues common to all Class members' claims relating to the Defendants Data Breach. By contrast, the class action device presents far fewer management difficulties and provides the benefit of a single adjudication, economies of scale, and comprehensive supervision by a single court.

34. The various claims asserted in this action are additionally or alternatively certifiable under the provisions of Federal Rules of Civil Procedure 23(b)(1) and/or 23(b)(2) because:

a. The prosecution of separate actions by millions of individual Class members would create a risk of inconsistent or varying adjudications with respect to individual Class members, thus establishing incompatible standards of conduct for Defendant;

b. The prosecution of separate actions by individual Class members would also create the risk of adjudications with respect to them that would, as a practical matter, be dispositive of the interests of the other Class members who are not a party to such adjudications and would substantially impair or impede the ability of such non-party Class members to protect their interests; and

c. Defendants acted or refused to act on grounds generally applicable to the entirety of each of the Class, thereby making appropriate final declaratory and injunctive relief with respect to the Class as a whole.

COUNT I
NEGLIGENCE

35. Plaintiff incorporates each paragraph of this Complaint as if set forth fully here, and further alleges as follows.

36. Defendants were, and continue to be, in confidential, special and/or fiduciary relationships with Plaintiff and Class Members by virtue of being entrusted with their personal information. At the very least, therefore, Defendants assumed a duty, and had duties imposed upon them by regulations, to use reasonable care to keep Plaintiff's

and Class Members' information private and secure, including a duty to comply with applicable PCI data security standards, statutes and/or regulations.

37. Defendants also had a duty to timely inform Plaintiff and Class Members of the breach and the fact that their personal information had been stolen and/or compromised, and, upon learning of the breach, a duty to take immediate action to protect Plaintiff and Class members from the foreseeable consequences of the breach. By their acts and omissions describes therein, Defendants unlawfully breached their duty, and Plaintiff and Class Members were harmed as a direct result.

38. Defendants knew, or should have known, that their system for processing and storing consumers' personal information had security vulnerabilities. Defendants were negligent by continuing to accept, process and store such information in light of these computer network vulnerabilities and the sensitivity of the personal information stored within.

39. The breach, and the resulting damages suffered by Plaintiff and Class Members, were the direct and proximate result of a number of actions and omissions, including but not limited to:

a. Defendants' improper retention and storage of Plaintiff's and Class Members' personal information;

b. Defendants' failure to use reasonable care to implement and maintain appropriate security procedures reasonably designed to protect such information;

c. Defendants' delay in notifying Plaintiff and Class Members about the breach for more than a year; and

d. Defendants' failure to take immediate and effective action to protect Plaintiff and Class members from potential and foreseeable damage.

40. Defendants' wrongful actions constitute negligence.

41. When Defendants gathered and transmitted consumers' personal information, they came into the possession, custody and control of this sensitive information and as such, were and continue to be in confidential, special and/or fiduciary relationships with Plaintiff and Class Members. At the very least, Defendants had a duty to monitor and safeguard such information to keep it private and secure, including a duty to ensure that Defendants complied with applicable PCI data security standards, statutes and/or regulations.

42. Defendants knew, or should have known, that their network for processing and storing consumers' personal information had security vulnerabilities. Defendants were negligent in continuing to process such information in light of those vulnerabilities and the sensitivity of the information.

43. The breach was a direct and/or proximate result of Defendants' failure to use reasonable care to ensure that they maintained appropriate security procedures reasonably designed to protect Plaintiff's and Class Members' personal information. Defendants' wrongful conduct constitutes negligence.

44. Plaintiff and Class Members have not in any way contributed to the security breach or the compromise or theft of their personal information.

COUNT II
NEGLIGENCE PER SE

45. Plaintiff incorporates each paragraph of this Complaint as if set forth fully here, and further alleges as follows.

46. Pursuant to the Gramm-Leach-Bliley Act (the "Act"), 15 U.S.C. § 6801, and related California consumer data protection statutes, Defendants had a duty to protect and keep consumers' personal information secure, private and confidential.

47. Defendants violated these Acts by not adequately safeguarding Plaintiff's and Class Members' Sensitive Personal Information; and monitoring and ensuring that Defendants complied with PCI data security standards, card association standards, statutes and/or regulations designed to protect such information.

48. Defendants also failed to comply with PCI data security standards, statutes and regulations prohibiting the storage of unprotected personal information.

49. Defendants' failure to comply with these Acts, industry standards and/or regulations constitutes negligence per se.

COUNT III
BREACH OF CONTRACT

50. Plaintiff incorporates each paragraph of this Complaint as if set forth fully here, and further alleges as follows.

51. Plaintiff and Class Members were parties to actual or implied contracts with Defendants that required Defendants to properly safeguard their personal information from theft, compromise and/or unauthorized disclosure.

52. Additionally, Plaintiff and Class Members were third party beneficiaries to contracts and/or agreements by and between Defendants and other institutions and networks. These agreements required Defendants to properly safeguard personal information from theft, compromise and unauthorized disclosure.

53. Defendants breached their agreements with Plaintiff and Class Members by failing to properly safeguard personal information from theft, compromise and/or unauthorized disclosure. Defendants' wrongful conduct constitutes breach of contract.

54. Defendants owed a duty to Plaintiff and the Nationwide Class to exercise reasonable care in obtaining, retaining, and safeguarding their Personal Data.

COUNT IV
BREACH OF CONSUMER PROTECTION STATUTES

55. Plaintiff incorporates each paragraph of this Complaint as if set forth fully here, and further alleges as follows.

56. Plaintiff brings this Count individually, and on behalf of all similarly situated residents of each of the 50 States and the District of Columbia, for violations of the respective statutory consumer protection laws of these States and territories, as follows:

a. Alabama Deceptive Trade Practices Act, Ala.Code 1975, § 8–19–1, *et seq.*;

b. Alaska Unfair Trade Practices and Consumer Protection Act, AS § 45.50.471, *et seq.*;

c. Arizona Consumer Fraud Act, A.R.S §§ 44-1521, *et seq.*;

d. Arkansas Deceptive Trade Practices Act, Ark.Code §§ 4-88-101, *et seq.*;

e. Colorado Consumer Protection Act, C.R.S.A. §6-1-101, *et seq.*;

f. Connecticut Unfair Trade Practices Act, C.G.S.A. § 42-110, *et seq.*;

g. Delaware Consumer Fraud Act, 6 Del. C. § 2513, *et seq.*;

h. D.C. Consumer Protection Procedures Act, DC Code § 28-3901, *et seq.*;

i. Florida Deceptive and Unfair Trade Practices Act, FSA §501.201, *et seq.*;

j. Georgia Fair Business Practices Act, OCGA § 10-1-390, *et seq.*;

k. Hawaii Unfair Competition Law, H.R.S. § 480-1, *et seq.*;

l. Idaho Consumer Protection Act, I.C. § 48-601, *et seq.*;

m. Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 501/1, *et seq.*;

n. Indiana Deceptive Consumer Sales Act, IN ST § 24-5-0.5-2, *et seq.*;

o. Iowa Private Right of Action for Consumer Frauds Act, Iowa Code Ann. § 714H.1, *et seq.*;

p. Kansas Consumer Protection Act, K.S.A. § 50-623, *et seq.*;

q. Kentucky Consumer Protection Act, KRS 367.110, *et seq.*;

r. Louisiana Unfair Trade Practices and Consumer Protection Law, LSA-R.S. 51:1401, *et seq.*;

s. Maine Unfair Trade Practices Act, 5 M.R.S.A. § 205-A, *et seq.*;

t. Maryland Consumer Protection Act, MD Code, Commercial Law, § 13-301, *et seq.*;

u. Massachusetts Regulation of Business Practices for Consumers Protection Act, M.G.L.A. 93A, *et seq.*;

v. Michigan Consumer Protection Act, M.C.L.A. 445.901, *et seq.*;

w. Minnesota Prevention of Consumer Fraud Act, Minn. Stat. §325F.68, *et seq.*;

x. Mississippi Consumer Protection Act, Miss. Code Ann. § 75-24-1, *et seq.*;

y. Missouri Merchandising Practices Act, V.A.M.S. § 407, *et seq.*;

z. Montana Unfair Trade Practices and Consumer Protection Act of 1973, Mont. Code Ann. § 30-14-101, *et seq.*;

aa. Nebraska Consumer Protection Act, Neb.Rev.St. §§ 59-1601, *et seq.*;

bb. Nevada Deceptive Trade Practices Act, N.R.S. 41.600, *et seq.*;

cc. New Hampshire Regulation of Business Practices for Consumer Protection, N.H.Rev.Stat. § 358-A:1, *et seq.*;

dd. New Jersey Consumer Fraud Act, N.J.S.A. 56:8, *et seq.*;

ee. New Mexico Unfair Practices Act, N.M.S.A. §§ 57-12-1, *et seq.*;

ff. New York Consumer Protection from Deceptive Acts and Practices, N.Y. GBL (McKinney) § 349, *et seq.*;

gg. North Carolina Unfair and Deceptive Trade Practices Act, N.C. Gen Stat. § 75-1.1, *et seq.*;

hh. North Dakota Consumer Fraud Act, N.D. Cent.Code Chapter 51-15, *et seq.*;

ii. Ohio Consumer Sales Practices Act, R.C. 1345.01, *et seq.*;

jj. Oklahoma Consumer Protection Act, 15 O.S.2001, §§ 751, *et seq.*;

kk. Oregon Unlawful Trade Practices Act, ORS 646.605, *et seq.*;

ll. Pennsylvania Unfair Trade Practices and Consumer Protection Law, 73 P.S. § 201-1, *et seq.*;

mm. Rhode Island Deceptive Trade Practices Act, G.L.1956 § 6-13.1-5.2(B), *et seq.*;

nn. South Carolina Unfair Trade Practices Act, SC Code 1976, §§39-5-10, *et seq.*;

oo. South Dakota Deceptive Trade Practices and Consumer Protection Act, SDCL § 37-24-1, *et seq.*;

pp. Tennessee Consumer Protection Act, T.C.A. § 47-18-101, *et seq.*;

qq. Texas Deceptive Trade Practices-Consumer Protection Act, V.T.C.A., Bus. & C. § 17.41, *et seq.*;

rr. Utah Consumer Sales Practices Act, UT ST § 13-11-1, *et seq.*;

ss. Vermont Consumer Fraud Act, 9 V.S.A. § 2451, *et seq.*;

tt. Virginia Consumer Protection Act of 1977, VA ST § 59.1-196, *et seq.*;

uu. Washington Consumer Protection Act, RCWA 19.86.010, *et seq.*;

vv. West Virginia Consumer Credit And Protection Act, W.Va.Code § 46A-1-101, *et seq.*;

ww. Wisconsin Deceptive Trade Practices Act, WIS.STAT. § 100.18, *et seq.*; and

xx. Wyoming Consumer Protection Act, WY ST § 40-12-101, *et seq.*

57. Defendants violated the statutes set forth above (collectively, the "Consumer Protection Acts") by failing to properly implement adequate, commercially reasonable security measures to protect Plaintiff's and Class Members' personal information, and by allowing third parties to access Plaintiff's and Class Members' personal information.

58. Defendants further violated the Consumer Protection Acts by failing to disclose to the consumers that their data security practices were inadequate, thus inducing consumers to schedule and book rides through Defendants.

59. Defendants' acts and/or omissions constitute fraudulent, deceptive, and/or unfair acts or omissions under the Consumer Protection Acts.

60. Plaintiff and Class Members were deceived by Defendants' failure to properly implement adequate, commercially reasonable security measures to protect their personal information.

61. Defendants intended for Plaintiff and Class Members to rely on Defendants to protect the information furnished to it in connection with debit and credit card transactions and/or otherwise collected by Defendants, in such manner that Plaintiff's and

Class Members' personal information would be protected, secure and not susceptible to access from unauthorized third parties.

62. Defendants instead handled Plaintiff's and Class Members' personal information in such manner that it was compromised.

63. Defendants failed to follow industry best practices concerning data security or was negligent in preventing the data breach from occurring.

64. It was foreseeable that Defendants' willful indifference or negligent course of conduct in handling personal information they collected would put that information at the risk of compromise by hackers.

65. On information and belief, Defendants benefited from mishandling the personal information of their customers, by not taking effective measures to secure this information, and therefore saving on the cost of providing data security.

66. Defendants' fraudulent and deceptive acts and omissions were intended to induce Plaintiff and Class Members' reliance on Defendants' deception that their personal information was secure.

67. Defendants' conduct offends public policy and constitutes unfair acts or practices under the Consumer Protection Acts because Defendants caused substantial injury to Plaintiff and Class Members that is not offset by countervailing benefits to consumers or competition, and is not reasonably avoidable by consumers.

68. Defendants' practices of choosing to not implement reasonable and appropriate security measures to protect their customers' and employees' personal information constitute violations of the Federal Trade Commission Act, 15 U.S.C.

§ 45(a), which the courts consider when evaluating claims under the Consumer Protection Acts, including 815 ILCS 505/2.

69. Defendants' conduct constitutes unfair acts or practices as defined in the Consumer Protection Acts because Defendants caused substantial injury to Plaintiff and Class Members, which injury is not offset by countervailing benefits to consumers or competition and was not reasonably avoidable by consumers.

70. Plaintiff and Class Members have suffered injury in fact and actual damages including lost money and property as a result of Defendants' violations of the Consumer Protection Acts.

71. Defendants' fraudulent and deceptive behavior proximately caused Plaintiff and Class Members' injuries, and Defendants conducted themselves with reckless indifference toward the rights of others, such that an award of punitive damages is appropriate.

72. Defendants' failure to disclose information concerning the Data Breach directly and promptly to affected customers and employees, constitutes a separate fraudulent act or practice in violation of the Consumer Protection Acts.

73. Plaintiff seeks attorney's fees and damages to the fullest extent permitted under the Consumer Protection Acts, including N.Y. G.B.L. § 349(h).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all others similarly situated, prays for judgment against Defendants as follows:

A. An Order certifying the Class and any appropriate subclasses thereof under the appropriate provisions of Federal Rule of Civil Procedure 23, and appointing Plaintiff and their counsel to represent the Class;

B. Declarations that the actions of Defendants, as set out above, are unlawful;

C. Appropriate injunctive and equitable relief, including, but not limited to, provision of credit monitoring services for a period of time to be determined by the trier-of-fact;

D. Compensatory damages;

E. Punitive damages;

F. Statutory damages;

G. Costs, disbursements, expenses, and attorneys' fees;

H. Pre- and post-judgment interest, to the extent allowable; and

I. Such other and further relief as this Court deems just and proper.

JURY DEMAND

Plaintiff, on behalf of himself and all others similarly situated, hereby demands a trial by jury in this case as to all issues so triable.

Dated: January 16, 2018

Respectfully submitted,

s/ Daniel C. Hedlund

Daniel E. Gustafson (#202241)
Daniel C. Hedlund (#258337)
Joseph C. Bourne (#389922)
Eric S. Taubel (#392491)
Kaitlyn L. Dennis (#397433)
GUSTAFSON GLUEK PLLC
Canadian Pacific Plaza
120 South Sixth Street, Suite 2600

Minneapolis, MN 55402
Telephone: (612) 333-8844
Facsimile: (612) 339-6622
Email: dgustafson@gustafsongluek.com
dhedlund@gustafsongluek.com
jbourne@gustafsongluek.com
etaubel@gustafsongluek.com
kdennis@gustafsongluek.com

ATTORNEYS FOR PLAINTIFF AND THE PROPOSED CLASS